РУКОВОДСТВО ПО НАСТРОЙКЕ ПОДКЛЮЧЕНИЯ К VPN СФУ ДЛЯ СТУДЕНТОВ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ SSL VPN

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ СФУ, 2021

Операционные системы семейства Windows

Перед настройкой данного типа подключения для операционных систем семейства Windows необходимо скачать и установить VPN-клиент.

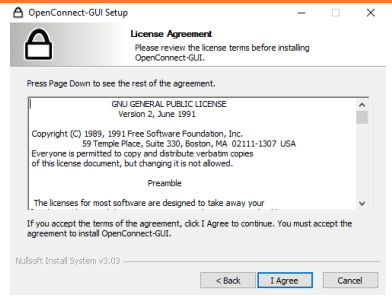
VPN-клиента можно скачать по следующей ссылке: https://users.sfu-kras.ru/files/openconnect-gui-1.5.3-win32.exe

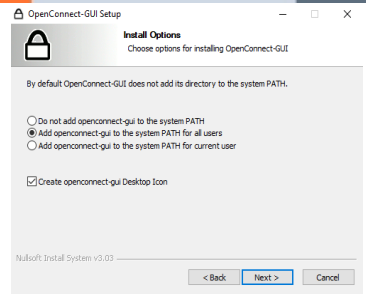
Так же можно воспользоваться любым VPN-клиентом, который поддерживает технологии Cisco AnyConnect или OpenConnect.

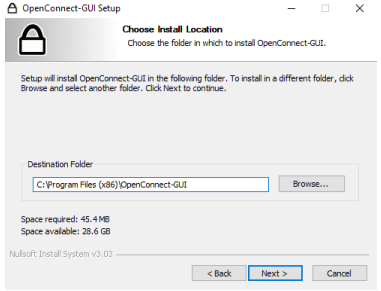
Операционные системы семейства Windows

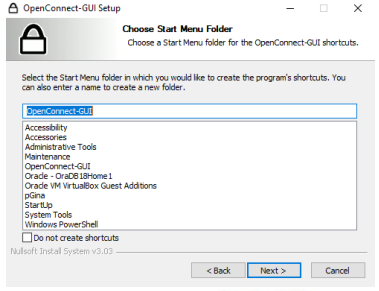
После того, как вы скачали VPN-клиент, необходимо его установить в вашу операционную систему.

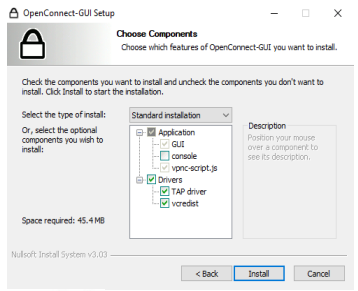
В процессе установке необходимо согласиться с условиями лицензионного соглашения, выбрать опции, которые позволят использовать подключение всем пользователям компьютера и создадут ярлык для быстрого запуска на рабочем столе. Путь установки, имя в стартовом меню и выбор компонентов можно оставить по умолчанию. В окне с предложением установить TAP-Windows адаптер выбираем "Install".
После этого установка VPN-клиента завершена, можно приступать к настройке подключения.

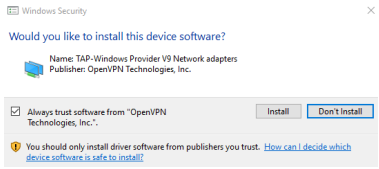


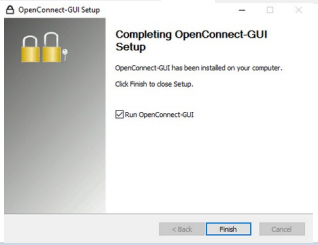




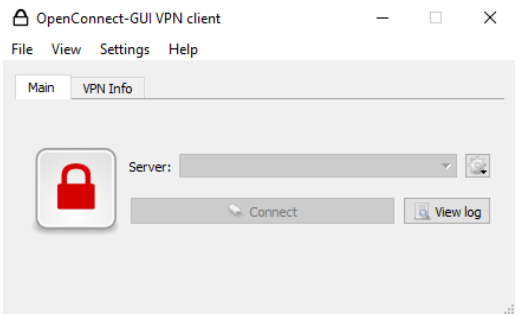


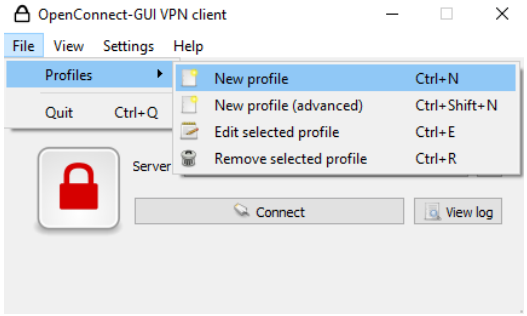


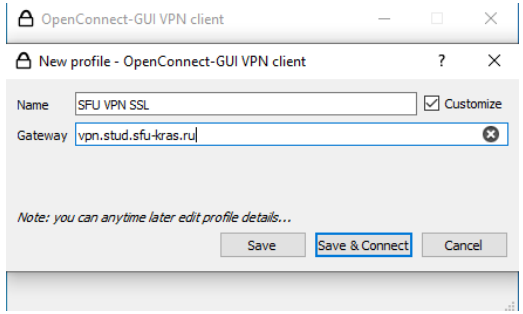


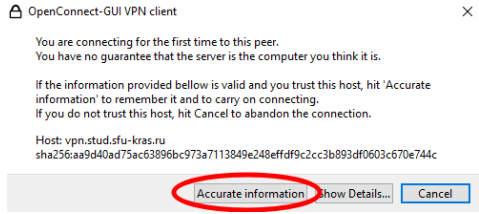


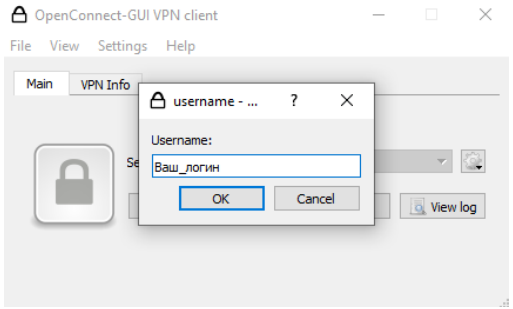
Операционные системы семейства Windows

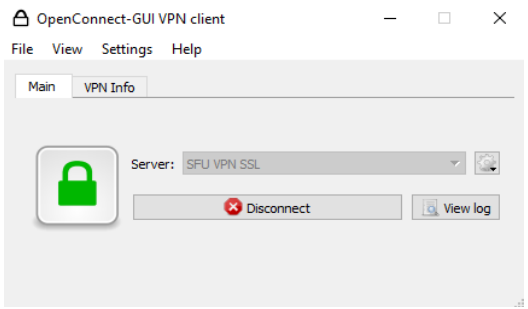












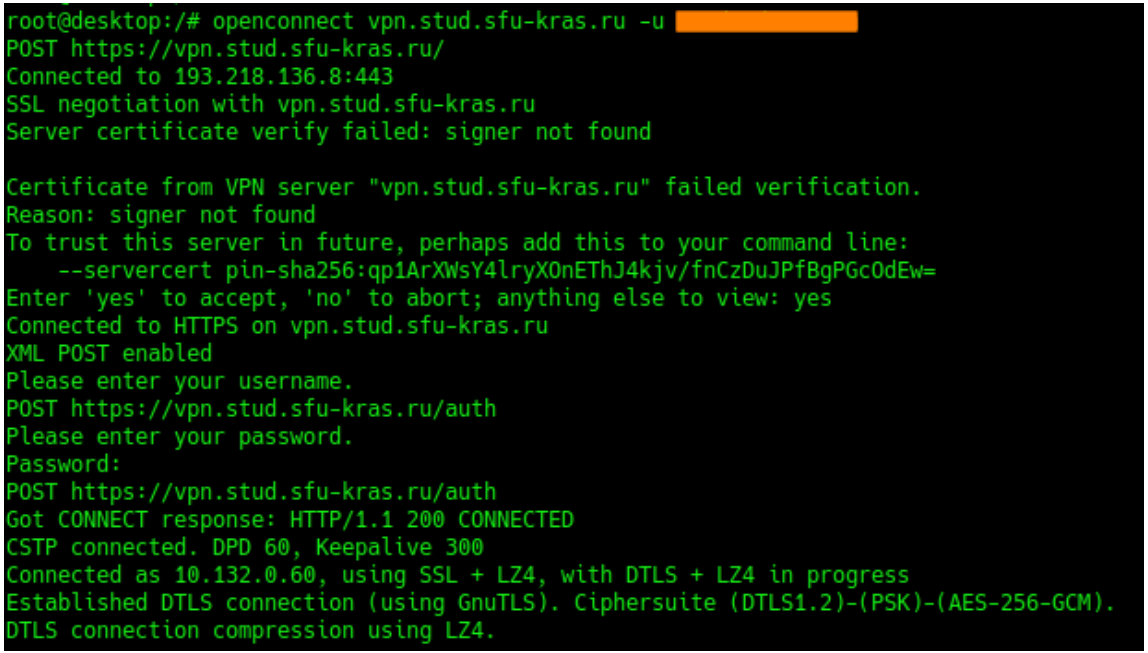
Процесс создания профиля подключения очень прост.
Вся последовательность показана на скриншотах.
Для успешного подключения необходимо указать:

- **Адрес сервера – vpn.stud.sfu-kras.ru**;
- **Ваш логин и пароль**.

Появление зеленого замка показывает успешное подключение к VPN-серверу.
Отключение от сервера происходит по нажатию кнопки "**Disconnect**".

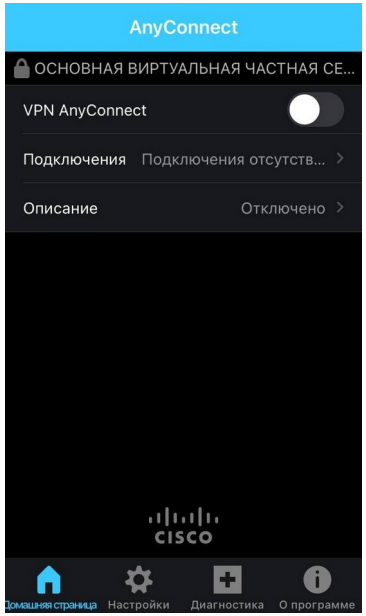
Операционные системы семейства Linux

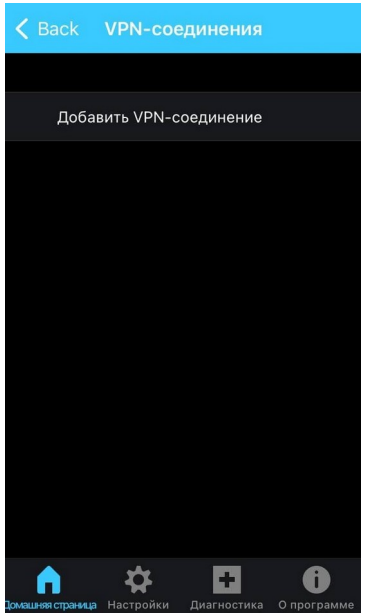
Для того, чтобы подключиться к VPN из ОС семейства Linux необходим пакет **openconnect**.
Для подключения без GUI используется команда **sudo openconnect -b vpn.stud.sfu-kras.ru -u LOGIN**, где -b перевод в фоновый режим, LOGIN – ваш логин.
Так как сертификат является самоподписанным, то необходимо ввести **yes** для его использования.
Разрыв соединения в этом случае производится командой **sudo pkill openconnect**.
Для создания профиля подключения через **Network-manager** необходимо установить соответствующие графической оболочке пакеты.

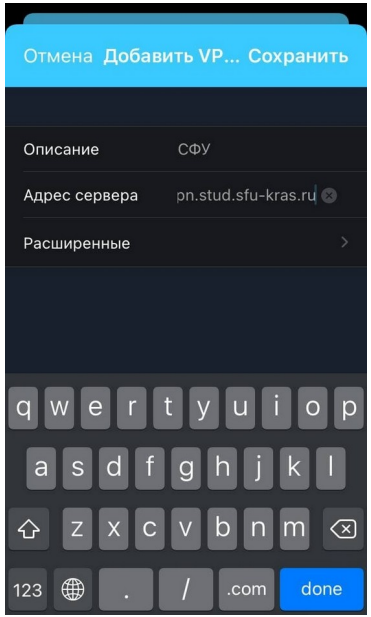


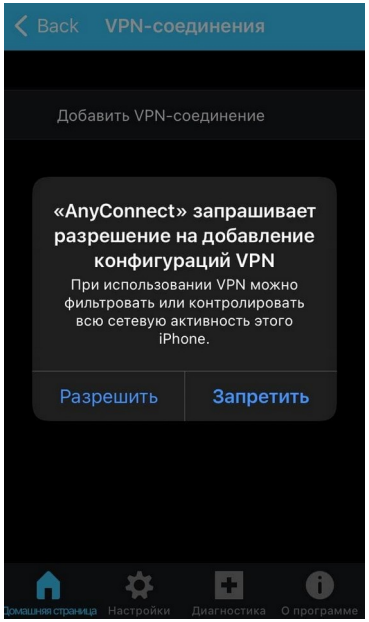
Операционные системы семейства IOS

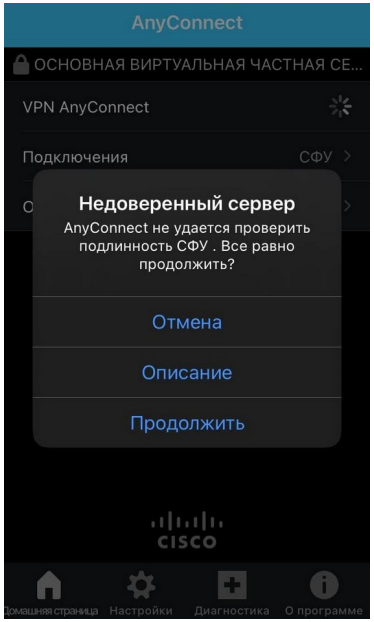
Для создания нового VPN-подключения необходимо установить приложение **Cisco AnyConnect** на ваше устройство. Создание профиля подключение показано на скриншотах ниже. Адрес сервера: **vpn.stud.sfu-kras.ru**. Необходимо **разрешить** добавить конфигурацию VPN и "**Продолжить**" при появлении сообщения о недоверенном сервере.





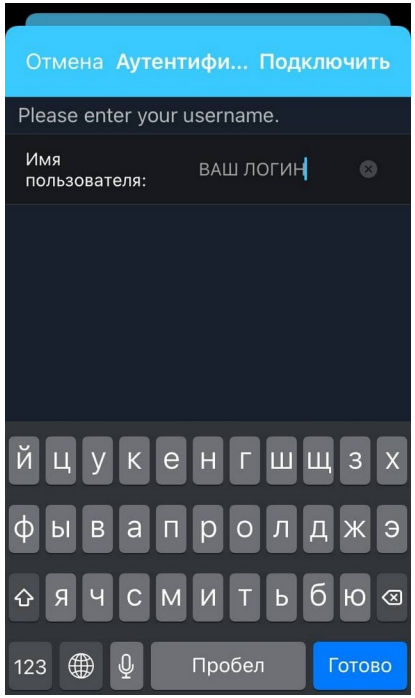


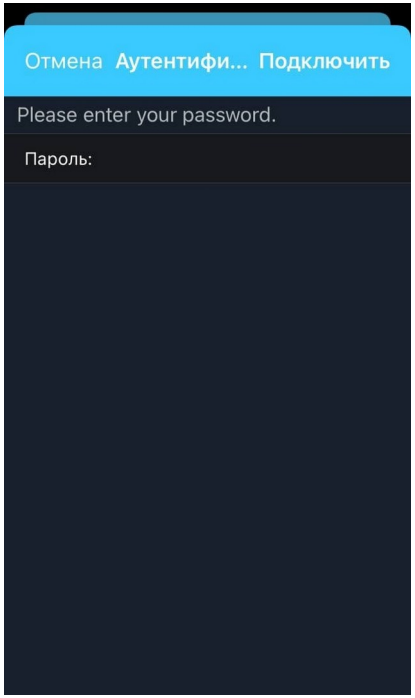


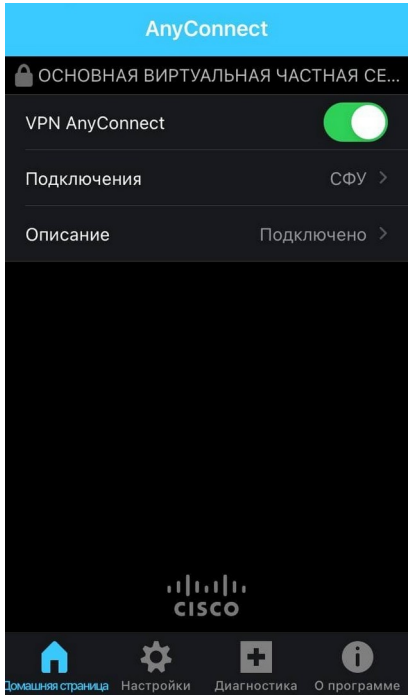


Операционные системы семейства IOS

В строке "**Имя пользователя"** указываем ваш логин, а в следующем окне указываем в строке "**Пароль**" ваш пароль.
После этого можно произвести подключение к VPN-серверу.
На некоторых устройствах также требуется отключить проверку сертификатов для данного сервера. В этом случае приложение перенаправит вас на страницу, где необходимо будет отключить проверку сертификата для сервера.
Самоподписанный сертификат сервера не является какой-либо уязвимостью или вредоносным ПО, ваше соединение будет зашифровано так же надежно, как и при использовании коммерческого сертификата.

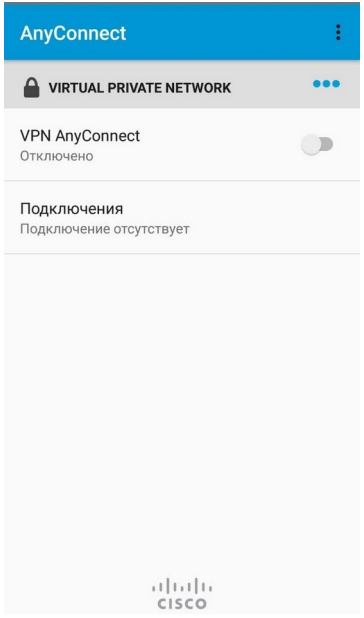


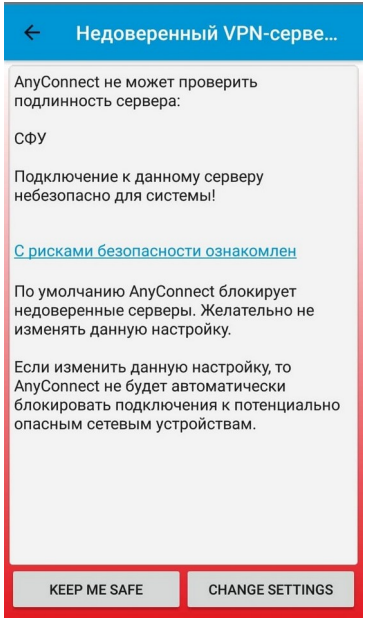


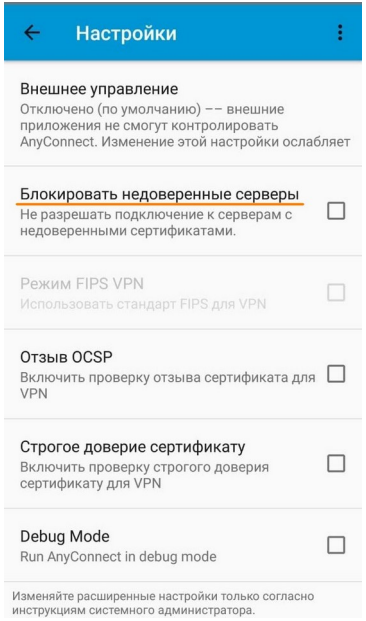


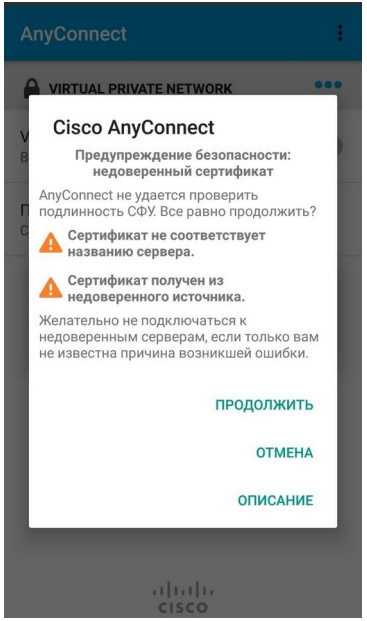
Операционные системы семейства Android

Для создания нового VPN-подключения необходимо установить приложение **Cisco AnyConnect** на ваше устройство. Создание профиля подключение показано на скриншотах ниже. Адрес сервера: **vpn.stud.sfu-kras.ru**. Необходимо изменить настройки безопасности нажав на "**CHANGE SETTINGS**" и отключить пункт "**Блокировать недоверенные серверы**". На появившемся предупреждении нажать "**ПРОДОЛЖИТЬ**".



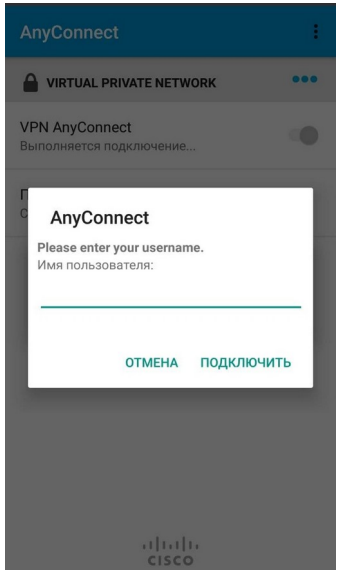


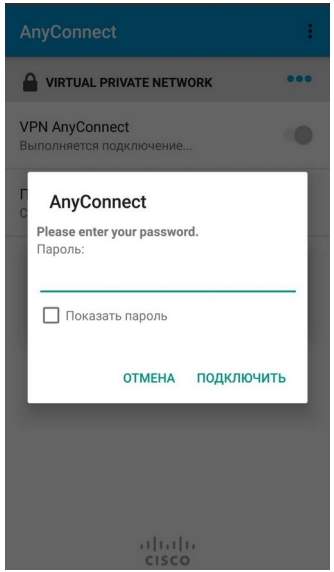


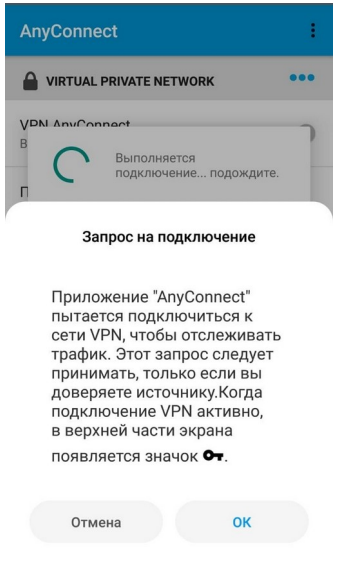


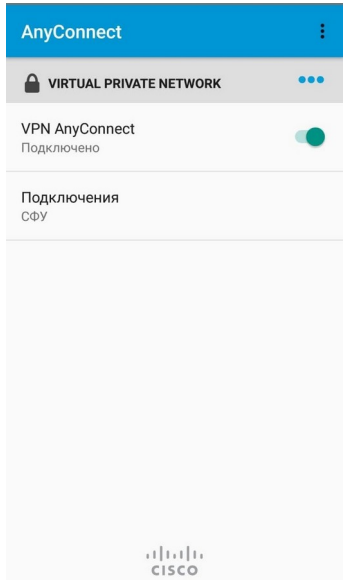
Операционные системы семейства Android

В строке "**Имя пользователя"** указываем ваш логин, а в следующем окне указываем в строке "**Пароль**" ваш пароль.
После этого можно произвести подключение к VPN-серверу.
На запрос на подключение отвечает утвердительно. После этого соединение будет утсановлено.
Самоподписанный сертификат сервера не является какой-либо уязвимостью или вредоносным ПО, ваше соединение будет зашифровано так же надежно, как и при использовании коммерческого сертификата.



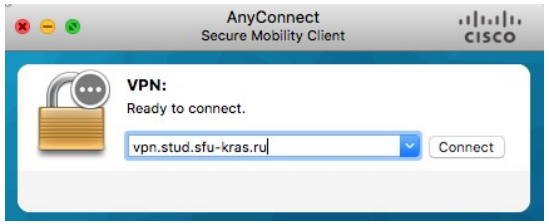


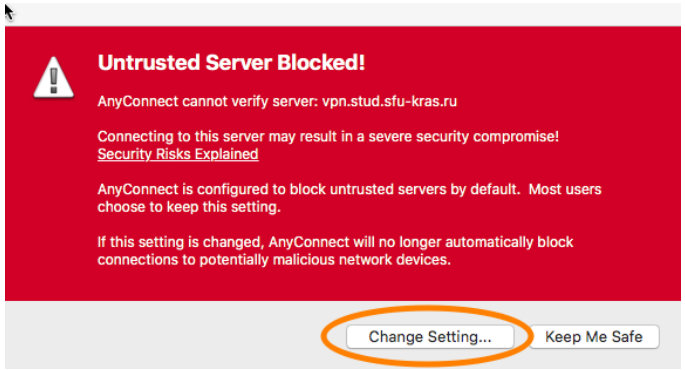


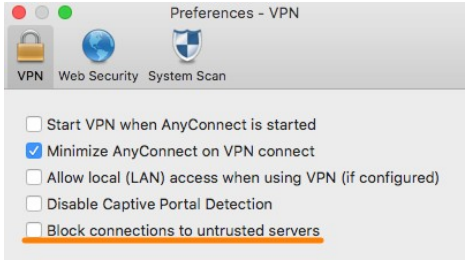


Операционные системы семейства macOS

Для создания нового VPN-подключения необходимо установить приложение **Cisco AnyConnect** на ваше устройство. Создание профиля подключение показано на скриншотах ниже. Адрес сервера: **vpn.stud.sfu-kras.ru**. Необходимо изменить настройки безопасности нажав на "**CHANGE SETTINGS**" и отключить пункт "**Block connections to untrusted servers**". На появившемся предупреждении нажать "**Connect Anyway**".







Операционные системы семейства macOS

В строке "**Username"** указываем ваш логин, а в следующем окне указываем в строке "**Password**" ваш пароль.
После этого можно произвести подключение к VPN-серверу.
На запрос на подключение отвечает утвердительно. После этого соединение будет утсановлено.
Самоподписанный сертификат сервера не является какой-либо уязвимостью или вредоносным ПО, ваше соединение будет зашифровано так же надежно, как и при использовании коммерческого сертификата.